

Release Notes

HP StorageWorks Secure Path 3.0C Service Pack 3 for Linux and Linux Workgroup Edition

Product Version: 3.0C SP3

Tenth Edition (March 2006)

Part Number: T3575-96501

This document summarizes characteristics of HP StorageWorks Secure Path 3.0C Service Pack 3 for Linux systems. For the latest version of these release notes, access the HP storage web site:
<http://www.hp.com/country/us/eng/prodserv/storage.html>.



© Copyright 2003–2006 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Linux is a U.S. registered trademark of Linus Torvalds.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in U.S.

Secure Path 3.0C Service Pack 3 for Linux and Linux Workgroup Edition Release Notes
Tenth Edition (March 2006)
Part Number: T3575-96501

About this document

This section describes the content reflected in this document, including:

- [Release notes information](#), page 3
- [Intended audience](#), page 3
- [Related documentation](#), page 4

Release notes information

These release notes describes the following:

- [Secure Path 3.0C SP3 kit contents](#), page 5
- [Secure Path support matrix](#), page 6
- [Updating to Secure Path 3.0C SP3](#), page 8
- [General notes](#), page 11
- [Red Hat Enterprise Linux 2.1 AS operating system notes](#), page 14
- [Red Hat Enterprise Linux 3.0 AS operating system notes](#), page 15
- [MSA1000 system notes](#), page 16
- [Cluster system notes](#), page 18
- [Known problems](#), page 21

Intended audience

This document is intended for customers who have purchased HP StorageWorks Secure Path 3.0x for Linux and Linux Workgroup Edition, and who are responsible for installing, configuring, and maintaining this product in their Linux server environment, assuming that you are familiar with Linux system administration, including hardware and software installation. The document is also intended for customers who want to upgrade to version 3.0C SP3 with any one of the following StorageWorks RAID Arrays:

- EVA3000 (version 3.020, 3.025) (HSV100)
- EVA5000 (version 3.020, 3.025) (HSV110)
- MSA1000 (version 4.32)
- MSA1500 (version 4.82) (Standalone only. Not supported in clusters)

Note: Read the *HP StorageWorks Secure Path 3.0C for Linux and Linux Workgroup Edition installation and reference guide* to ensure that all pre-installation requirements are met.

Related documentation

Additional documentation that you may find helpful includes:

- *HP StorageWorks Secure Path 3.0C for Linux and Linux Workgroup Edition installation and reference guide*, part number AA-RU7VD-TE
- HP StorageWorks Command View EVA help file
- SteelEye LifeKeeper for Linux documentation:
<http://licensing.steeleye.com/support/docm.php>
- White papers and best practices documents is available on the HP web site:
<http://www.hp.com/country/us/eng/prodserv/storage.html>
- HP Serviceguard for Linux documentation:
<http://www.hp.com/servers/proliant/ha/serviceguard/info>

Secure Path 3.0C SP3 kit contents

The Secure Path 3.0C SP3 for Linux and Linux Workgroup Edition kit includes:

- *HP StorageWorks Secure Path 3.0C for Linux and Linux Workgroup Edition installation and reference guide*, part number AA-RU7VD-TE
- *HP StorageWorks Secure Path 3.0C SP1 for Linux and Linux Workgroup release notes*, part number T3575-96301.
- *HP StorageWorks Secure Path 3.0C SP2 for Linux and Linux Workgroup release notes*, part number T3575-96401.
- *HP StorageWorks Secure Path 3.0C SP3 for Linux and Linux Workgroup release notes*, part number T3575-96501 (this document).

Secure Path support matrix

Table 1 lists the hardware and software supported by Secure Path for Linux and Linux Workgroup Edition.

Table 1: Secure Path supported hardware and software

Host feature	Supported hardware and software	
Operating system	Red Hat Enterprise Linux 2.1 Update 6, AS 32-bit 2.4.9-e.59smp Red Hat Enterprise Linux 2.1 Update 6, AS/ES 32-bit 2.4.9-e.59enterprise Red Hat Enterprise Linux 2.1 Update 6, AS 64-bit 2.4.18-e.52smp Red Hat Enterprise Linux 2.1 Update 7, AS 32-bit 2.4.9-e.62smp Red Hat Enterprise Linux 2.1 Update 7, AS/ES 32-bit 2.4.9-e.62enterprise Red Hat Enterprise Linux 2.1 Update 7, AS 64-bit 2.4.18-e.56smp Red Hat Enterprise Linux 3.0 Update 6, AS 32-bit 2.4.21-37.ELsmp Red Hat Enterprise Linux 3.0 Update 6,hugemem, AS 32-bit 2.4.21-37.ELhugemem Red Hat Enterprise Linux 3.0 Update 6, AS 64-bit 2.4.21-37.EL Red Hat Enterprise Linux 3.0 Update 7, AS 32-bit 2.4.21-40.ELsmp Red Hat Enterprise Linux 3.0 Update 7,hugemem, AS 32-bit 2.4.21-40.ELhugemem Red Hat Enterprise Linux 3.0 Update 7, AS 64-bit 2.4.21-40.EL SuSE LINUX Enterprise Server 8/UnitedLinux 1.0, SP3, 32-bit: 2.4.21-273-smp SuSE LINUX Enterprise Server 8/UnitedLinux 1.0, SP4, 32-bit: 2.4.21-304-smp SuSE LINUX Enterprise Server 8/UnitedLinux 1.0, SP3, 64-bit: 2.4.21-273-itanium2-smp SuSE LINUX Enterprise Server 8/UnitedLinux 1.0, SP4, 64-bit: 2.4.21-304-itanium2-smp For information about the latest kernel support, access the following web site: http://www.hp.com/go/securepath	
Platform software kit	MSA1000 MSA 1500 EVA3000 EVA5000	MSA1000 Support Software, V4.32 MSA 1500 Support Software, V4.82 Linux 3.0C for Enterprise Virtual Array Linux 3.0C for Enterprise Virtual Array
RAID storage systems	StorageWorks EVA5000 (VCS version 3020, 3025), EVA3000 (VCS version 3020, 3025), MSA1000 version4.32, MSA1500 version4.82.	
Host Bus Adapters (HBA)	FCA2214/FCA2214DC 2-Gb PCI-X and A6826A, driver version 7.07.03-14/8.01.03-14	

Table 1: Secure Path supported hardware and software (Continued)

Host feature	Supported hardware and software	
Clusters	MSA1000, EVA3000, EVA5000	<p>SteelEye LifeKeeper for Linux 4.6.1 for 32-bit systems only. Red Hat 2.1 and SuSE LINUX Enterprise Server 8 only</p> <p>HP Serviceguard for Linux:</p> <p>A.11.14 for any Red Hat Enterprise Linux 2.1 Updates</p> <p>A.11.15 and A.11.16 for Red Hat Enterprise Linux 3.0 Update 3 or later</p> <p>A.11.15 for SUSE Linux Enterprise Server 8/UnitedLinux 1.0, SP3/SP4</p>
Logical volume manager	Native OS support	
Fibre channel SAN switches	<p>Refer to the HP StorageWorks SAN Design reference guide for configuration information about Fibre Channel switches support. This document is available on the HP web site:</p> <p>http://h18004.www1.hp.com/products/storageworks/san/documentation.html</p>	

Note: HSG80 controllers are not supported in this release.

Updating to Secure Path 3.0C SP3

This section describes the updated RedHat Package Manager (RPMs) and requirements for 32-bit or 64-bit operating systems:

- [32-bit systems](#), page 8
- [64-bit systems](#), page 9

Refer to chapter 5 in the *HP StorageWorks Secure Path 3.0C for Linux and Linux Workgroup Edition installation guide* for specific updating instructions.

Note: Because there is no commercial update process at this time for updating Red Hat Enterprise Linux 2.1 to Red Hat Enterprise Linux 3.0, or for updating SUSE LINUX 7/UnitedLinux 1.0 to SUSE LINUX 8/UnitedLinux 1.0, you must follow the update procedures described in either “[32-bit systems](#)” on page 8 or “[64-bit systems](#)” on page 9.

- Updating these systems requires a complete installation, which deletes all files on the hard disk.
 - If a previous version of Secure Path is installed, the update solution saves all configuration files and then updates the Secure Path software to 3.0C SP3.
-

32-bit systems

The system does not require previous installations of Secure Path (3.0, 3.0A, 3.0B, or 3.0C) for a successful update. However, Secure Path 3.0, 3.0A, 3.0B, or 3.0C RPM must be located in the `/tmp/securepathRPM` directory so that the update gets validated.

To update from Secure Path 3.0, 3.0A, 3.0B, or 3.0C to Secure Path 3.0C SP3, ensure that you have the following RPMs in the `/tmp/securepathRPM` directory.

Table 2: Secure Path 3.0C SP3 32-bit update RPMs

To update this RPM:	Use:
Secure-Path-3.0-8.0.noarch.rpm	Secure-Path-3.0CFullUpdate-4.0.SP3
Secure-Path-3.0AFull-4.0.noarch.rpm	Secure-Path-3.0CFullUpdate-4.0.SP3
Secure-Path-3.0BFull-5.0.noarch.rpm	Secure-Path-3.0CFullUpdate-4.0.SP3
Secure-Path-3.0CFull-4.0.noarch.rpm	Secure-Path-3.0CFullUpdate-4.0.SP3
Secure-Path-3.0c-8.0.noarch.rpm	Secure-Path-3.0CwkgUpd-4.0.SP3

Table 2: Secure Path 3.0C SP3 32-bit update RPMs

To update this RPM:	Use:
Secure-Path-3.0Ac-4.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate-4.0.SP3
Secure-Path-3.0Bc-5.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate-4.0.SP3
Secure-Path-3.0Cwkgrp-4.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate-4.0.SP3

64-bit systems

If you are updating from Secure Path 3.0C (for Linux or Linux Workgroup) to Secure Path 3.0C SP3 (for Linux or Linux Workgroup), you can access the update kit at the following web site:

<http://h18000.www1.hp.com/products/sanworks/secure-path/index.html>

The system does not require previous installations of Secure Path 3.0C for a successful update. However, the Secure Path 3.0C RPM must be located in the /tmp/securepathRPM directory so the update gets validated.

Table 3 lists the update RPMs for 64-bit systems in this release of Secure Path.

Table 3: Secure Path 3.0C SP3 64-bit update RPMs

For this operating system:	To update this RPM:	Use:
Red Hat	Secure-Path-3.0BFull64-4.0.noarch.rpm	Secure-Path-3.0CFull64Update-4.0.SP3
SUSE/ UnitedLinux	Secure-Path-3.0BFullSuse64-4.0.noarch.rpm	Secure-Path-3.0CFullUL64Update-4.0.SP3
Red Hat	Secure-Path-3.0CFull64-4.0.noarch.rpm	Secure-Path-3.0CFull64Update-4.0.SP3
SUSE/ UnitedLinux	Secure-Path-3.0CFullUL64-4.0.noarch.rpm	Secure-Path-3.0CFullUL64Update-4.0.SP3
Red Hat	Secure-Path-3.0Bc64-4.0.noarch.rpm	Secure-Path-3.0Cwkgrp64Update-4.0.SP3

Table 3: Secure Path 3.0C SP3 64-bit update RPMs

For this operating system:	To update this RPM:	Use:
SUSE/ UnitedLinux	Secure-Path-3.0BcSuse64-4.0.noarch.rpm	Secure-Path-3.0CwkgrpUL64Update-4.0.SP3
Red Hat	Secure-Path-3.0CFull64-4.0.noarch.rpm	Secure-Path-3.0CFull64Update-4.0.SP3
SUSE/ UnitedLinux	Secure-Path-3.0CFullUL64-4.0.noarch.rpm	Secure-Path-3.0CFullUL64Update-4.0.SP3

Note: For SUSE/UnitedLinux RPMs, the RPM name has changed from FullSuse64 to FullUL64.

General notes

This section describes the following:

- [Secure Path Manager](#), page 11
- [Module placement](#), page 11
- [RPM installation conditions](#), page 11
- [Licensing messages](#), page 12
- [Disconnecting cables](#), page 12
- [Linux distributions](#), page 12
- [Unsupported uni-processor kernels](#), page 12
- [Removing a disk](#), page 13
- [LUN limitations](#), page 13
- [Removing Secure Path RPM](#), page 13

Secure Path Manager

This release includes the Secure Path Manager `spmgr passwd` command, which lets you change the Secure Path default password to a unique password.

To enter a new password, use the following `spmgr passwd` command as follows:

```
spmgr passwd new_password
```

Module placement

Secure Path modules are now placed in the `/etc/CPQswsp/modules` directory.

RPM installation conditions

RPM checks for the following pre-installation conditions:

- SMP or enterprise kernel is loaded.
- The `qla2300` module is loaded.
- The kernel is a supported version.

If the pre-installation conditions are not met, the RPM exits. The RPM system generates an error message, as in the following example.

```
Error: execution of %pre scriptlet from Secure-path-30CFull-4.0
failed. exit status 255

Error: install %pre scriptlet failed (2). Skipping
Secure-path-30CFull-4.0
```

For more information, refer to the *HP StorageWorks Secure Path 3.0C for Linux and Linux Workgroup Edition installation and reference guide*.

Licensing messages

When booting your Linux system, you may see a message on the console similar to the following during Secure Path module load:

```
"....will taint the kernel no license"
```

You can safely ignore this message during a Secure Path module load, since newer versions of Linux check for GPL licenses (publicly licensed) during the module load and Secure Path is not GPL.

Disconnecting cables

HP does not recommend disconnecting Fibre Channel cables from one switch and connecting them to another switch while the system is running.

Linux distributions

Some Linux distributions ship with only 16 device nodes already created in `/dev`. If `ls /dev/sd*` does not display an entry, then you need to create the device nodes using the `/dev/MAKEDEV` script as follows:

```
/dev/MAKEDEV /dev/sd?
```

Replace the question mark (?) with the letter of the device.

Unsupported uni-processor kernels

Secure Path does not support uni-processor kernels. If you have a uni-processor system, you must run the SMP kernel to install Secure Path.

Removing a disk

Removing a disk under any circumstances causes all the paths to that device to be marked `standby`, and it causes the state of that LUN to be marked `dead`.

LUN limitations

Although Linux vendors support up to 128 LUNs, tests have shown that LUN limitations may vary. The maximum number of LUNs supported depends upon the vendor and revision of the kernel.

Note: The 128-LUN limit in Linux applies to the total number of LUNs as discovered by the low-level driver prior to Secure Path loading. In the case of a multi-path environment, this means that the actual LUN count will be less than 128.

Example: The basic setup involves one MSA1000 (2 paths per LUN) connected to one switch that is connected to the server by one single port adapter. The low-level driver sees each MSA1000 LUN twice (2 paths per LUN). Therefore, the maximum number of actual MSA1000 LUNS is limited to 64 ($64 \times 2 \text{ paths} = 128$).

Removing Secure Path RPM

If you remove the Secure Path RPM, reboot your system to ensure that the modules are unloaded properly. HP does not recommend removing Secure Path modules manually.

The following warning is displayed if you install and then immediately uninstall the Secure Path RPM:

```
/usr/sbin/makewhatis: cd: /usr/man: No such file or directory
```

This is because the `makewhatis` command does not have sufficient time to create or update the man page database.

You should not manually remove or reinstall the FCA2214/FCA2214 DC or the A6826A HBA driver or any platform kit while Secure Path is loaded.

Red Hat Enterprise Linux 2.1 AS operating system notes

You must install the `libgcc` library if you have loaded Red Hat Enterprise Linux 2.1 AS kernel.

You can get the `libgcc` library from either the Red Hat web site at <http://www.redhat.com> or the Red Hat Enterprise Linux AS2.1 CD-ROM.

Red Hat Enterprise Linux 3.0 AS operating system notes

Unlike 2.1, Red Hat Enterprise Linux 3.0 AS has the `libgcc` library installed. Therefore, you do not need to install the `libgcc` library when loading the kernel or when updating.

MSA1000 system notes

This section describes the following:

- [Failover on the MSA1000](#), page 16
- [Multiple servers sharing an MSA1000](#), page 16

Failover on the MSA1000

When a failover occurs on an MSA1000, all LUNs on the failed controller fail over to the active controller. However, when you run the `spmgr` utility and display the LUN state, any LUN that was not performing I/O appears not to have failed over to the newly active controller. This is normal and as soon as any I/O is attempted on one or more of these LUNs, it fails over and is displayed correctly.

Multiple servers sharing an MSA1000

This section describes the following:

- [Controller thrashing effect](#)
- [Only single-fault conditions are supported](#)

Controller thrashing effect

In an environment with multiple servers sharing an MSA1000, a thrashing effect may occur during reboots. You can ignore this effect if it occurs. Thrashing can be exacerbated when the `auto_restore` option is enabled.

The thrashing effect is defined as the MSA1000 controllers failing over and then failing back multiple times. This effect can occur if one or more of the servers sharing the MSA1000 is booted while other servers are online to the MSA1000. The cause is a combination of SCSI probing and the MSA1000 functional design.

Only single-fault conditions are supported

Secure Path 3.0C SP3 for Linux and Linux Workgroup Edition supports only single-fault conditions. On rare occasions, a double-fault condition can occur and unexpected behavior may result.

Examples of double-faults conditions are:

- A path failure occurs on one server (host A) in a multiple server configuration, and another server (host B) with at least two paths is rebooted. The result is I/O errors.

- All paths from one server in a cluster fail. The server may not fail over to another server in the cluster.

Cluster system notes

This section describes the following:

- [Cluster node limitations](#), page 18
- [LifeKeeper clusters with Secure Path in an EVA3000 or EVA5000 configuration](#), page 18

Cluster node limitations

Secure Path 3.0C SP3 has the following cluster code limitations:

- It supports only two-node clusters running SteelEye LifeKeeper for Linux or Serviceguard for Linux on SUSE Linux Enterprise Server 8/UnitedLinux 1.0.
- It does not support Red Hat 3.0.

LifeKeeper clusters with Secure Path in an EVA3000 or EVA5000 configuration

To ensure that a LifeKeeper cluster can properly run with Secure Path in a cluster using either an EVA3000 or EVA5000 as the storage array, you must use the following instructions:

- [Hardware configuration](#)
- [Software configuration](#)
- [Adding hosts to an EVA5000/EVA3000 cluster](#)

Hardware configuration

For physical dual-path configurations, complete the following procedure:

1. Create a zone that logically connects fabric port 1 of controller 1 to switch 1.
2. Create a zone that logically connects fabric port 1 of controller 2 to switch 2.

Note: Only one port per controller may be used in this configuration.

3. Connect Host Bus Adapter 1 to switch 1 for both servers 1 and 2.
4. Connect Host Bus Adapter 2 to switch 2 for both servers 1 and 2.

Figure 1 is an example of the logical dual-path configuration.

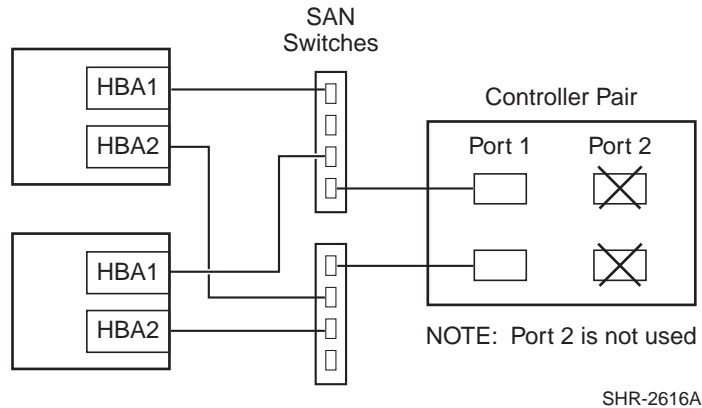


Figure 1: Logical dual-path configuration

Note: Port 2 is not part of the zoned configuration.

Software configuration

Note: This software configuration applies only to LifeKeeper for Linux. HP Serviceguard for Linux does not need a special configuration for Enterprise Virtual Array storage systems.

To install and configure Secure Path with HP Serviceguard for Linux or LifeKeeper for Linux in a two-node cluster, follow the instructions in related documentation and release notes. Refer to “[Related documentation](#)” on page 4 for additional information.

Adding hosts to an EVA5000/EVA3000 cluster

Complete the following procedure to add hosts to an EVA5000/EVA3000 running VCS 3.x:

1. Using Command View EVA, set the Host OS type to Custom instead of selecting Sun Solaris, as specified in the *HP StorageWorks Linux Kit 3.0E for Enterprise Virtual Array release notes*.

- Set the Custom Mode Number to 000000002200282E.

Refer to [Figure 2](#) for an example of setting your Host OS type and Custom Mode Number.

Note: You can configure Host OS as Custom only when adding a new host. If the host already exists, delete and re-add it before configuring the Host OS as Custom.

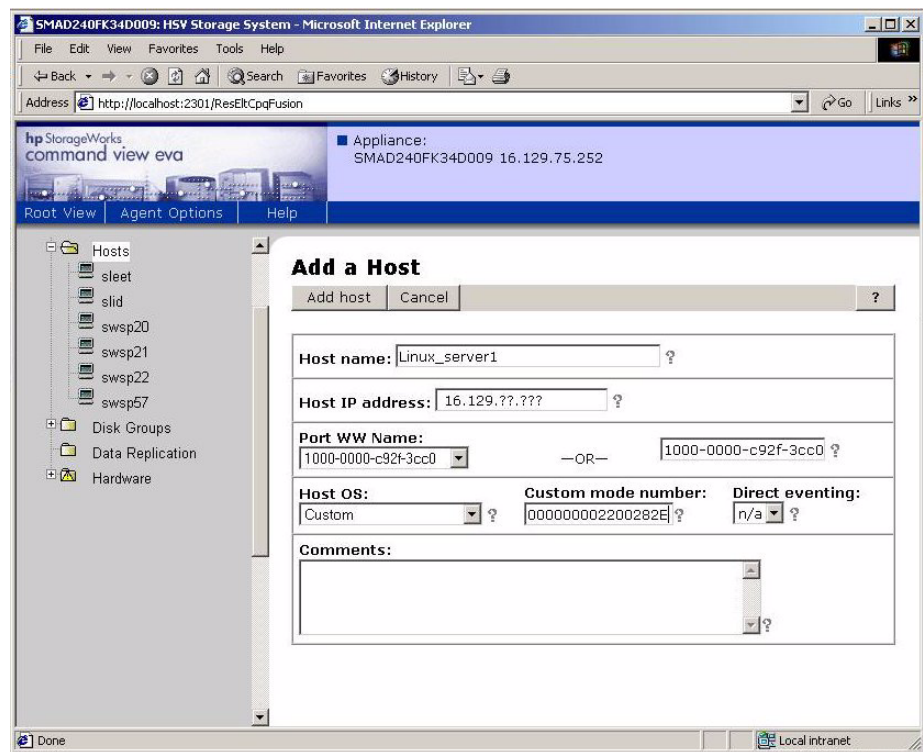


Figure 2: OS type and Custom mode number

Note: Refer to the *HP StorageWorks Command View EVA interactive help file* for more information on Command View EVA Add Host window.

Known problems

Following are the known problems of Secure Path 3.0C SP3 for Linux and Linux Workgroup Edition:

- Autorestore is not supported on the MSA1000 arrays.
- The `spmgr` command gets hanged if invalid arguments are entered.
- The `FAILED` path indication is not displayed when the MSA standby path is disconnected on SuSE LINUX Enterprise Server 8/UnitedLinux 1.0, SP3, SP4, and Red Hat Enterprise Linux 2.1 Update 6, 7.